Unofficial Translation

BANK INDONESIA

No. 14 / 38 /DASP Jakarta, 28 December 2012

CIRCULAR LETTER

to

ALL NON-BANK PROVIDERS
OF PAYMENT SYSTEM SERVICES
IN INDONESIA

Subject: Standard Guidelines for Implementation of the Anti-Money Laundering and Prevention of Terrorism Financing Programme for Non-Bank Providers of Payment System Services

In regard to the issuance of Bank Indonesia Regulation Number 14/3/PBI/2012 concerning the Anti-Money Laundering and Prevention of Terrorism Financing Programme for Non-Bank Providers of Payment System Services (State Gazette of the Republic of Indonesia Number 86 of 2012, Supplement to the State Gazette Number 5302), hereafter referred to as the AML and PTF BI Regulation, it is necessary to stipulate standard guidelines for implementation of the Anti-Money Laundering and Prevention of Terrorism Financing (AML and PTF) programme for Non-Bank Providers of Payment System Services as follows:

I. STANDARD GUIDELINES FOR IMPLEMENTATION OF THE AML AND PTF PROGRAMME

In accordance with the AML and PTF BI Regulation, each Non-Bank Provider of Payment System Services is required to formulate and submit written policies and procedures for implementation of

the ...

the AML and PTF programme to Bank Indonesia in the form of guidelines for implementation of the AML and PTF programme.

In formulating these guidelines for implementation of the AML and PTF programme, Non-Bank Providers of Payment System Services are required to apply the minimum standards stipulated in the Standard Guidelines for Implementation of the AML and PTF Programme as referred to in the Annex, which constitutes an integral part of this Circular Letter of Bank Indonesia.

Any Provider having obtained a licence from Bank Indonesia prior to the enactment of the AML and PTF BI Regulation is required to bring its Guidelines for Implementation of Know Your Customer Principles into conformity with these Standard Guidelines for Implementation of the AML and PTF Programme and submit these guidelines to Bank Indonesia no later than 3 (three) months after the entry into force of the AML and PTF BI Regulation, that is to say, 9 September 2013.

II. CONCLUDING PROVISIONS

The provisions of this Circular Letter of Bank Indonesia shall enter into force on 8 June 2013.

For the public to be informed, it is ordered that this Circular Letter of Bank Indonesia be promulgated in the State Gazette of the Republic of Indonesia.

Kindly be informed.

BANK INDONESIA,

BOEDI ARMANTO
HEAD OF THE DEPARTMENT
OF ACCOUNTING AND THE PAYMENT SYSTEM

CHAPTER I

INTRODUCTION

To prevent the exploitation of Non-Bank Providers of Payment System Services, encompassing issuers and/or acquires in Card-Based Payment Instrument (CBPI) activities, issuers and/or acquirers of Electronic Money (e-money) and/or providers of Remittance Services (RS), hereafter referred to as Providers, as vehicles for money laundering and/or terrorism financing, Providers are required to apply the Anti-Money Laundering and Prevention of Terrorism Financing (AML and PTF) programme as stipulated in Bank Indonesia Regulation No. 14/3/PBI/2012 concerning the Anti-Money Laundering and Prevention of Terrorism Financing Programme for Non-Bank Providers of Payment System Services (AML and PTF BI Regulation).

A. Money Laundering

1. Pursuant to Act No. 8 of 2012 concerning Prevention and Eradication of Money Laundering (AML Law):
   a. Money Laundering is any act that fulfils elements of criminal acts as stipulated in the provisions of the AML Law.
   b. Money laundering crimes are the acts of:
      1) placement, transfer, conversion, purchase, payment, grant, safe-keeping, carrying overseas, transformation, exchange for other currency or securities or other act in respect of Assets known or reasonably suspected to constitute proceeds of crime with the objective of concealing or disguising the origin of these assets.
      2) concealing or disguising the origin, source, location, intended use, transfer of rights or actual ownership of assets known or reasonably suspected to constitute proceeds of crime.

3) receiving …

3) receiving or controlling placements, transfers, payments, grants, donations, safe-keeping, exchange or use of assets known or reasonably suspected to constitute proceeds of crime. This provision does not apply to Reporting Parties who comply with the reporting requirements stipulated in the AML Law.

c. Proceeds of crime are Assets acquired from crimes as follows:

1) Corruption;
2) Bribery;
3) Narcotics;
4) Psychotropics;
5) smuggling of labour;
6) smuggling of migrants;
7) in banking;
8) in the capital market;
9) in insurance;
10) customs;
11) excise;
12) human trafficking;
13) illegal arms trade;
14) terrorism;
15) kidnapping;
16) theft;
17) embezzlement;
18) fraud;
19) currency counterfeiting;
20) gambling;
21) prostitution;
22) in taxation;
23) in forestry;
24) in the environment;
25) in marine affairs and fisheries; or

26) other …

26) other crimes punishable by imprisonment of 4 (four) years or more.

perpetrated in the territory of the Unitary State of the Republic of Indonesia or outside the territory of the Unitary State of the Republic of Indonesia and such crimes also constitute crimes under Indonesian law.

2. In essence, the processes of money laundering can be grouped into 3 (three) stages of activity, encompassing the following:
   a. Placement, i.e. placement of funds generated by a criminal activity into the financial system. Examples of placement in the provision of payment systems services include but are not limited to the following:
      1) Deposit of funds from the proceeds of crime with a Provider for conveyance to another party.
      2) Top up of Electronic Money by using the proceeds of crime.
   b. Layering is any effort to transfer assets originating from proceeds of crime that have successfully undergone placement into the financial system to further obscure the origin of these assets. The following are examples of layering in the operation of payment system services:
      1) Transfer of Electronic Money value originating from proceeds of crime.
      2) Ordering a Provider to transfer proceeds of crime to another party.
   c. Integration is any attempt to make use of purportedly legitimate assets, whether for immediate benefit, investment in various material or financial assets, use in financing legitimate business activity, or to be ploughed back into criminal activity.

3. Modes of money laundering commonly employed by money launderers are:

a. Smurfing ...

a. Smurfing, i.e. attempts to circumvent reporting by splitting transactions so that they are conducted by many parties.
b. Structuring, i.e. attempts to circumvent reporting by splitting transactions in order to reduce transaction amounts.
c. U turns, i.e. attempts to obscure the origin of proceeds of crime by conducting multiple transactions for subsequent return to the original sender.
d. Cuckoo smurfing, i.e. attempts to obscure the original source of funds by sending funds originating from proceeds of crime through third parties waiting for inward remittances and unaware that the funds received by them constitute proceeds of crime.
e. Use of third parties, i.e. transactions conducted with the use of third party identities for the purpose of avoiding detection of the identity of the actual parties who hold the funds from proceeds of crime.
f. Mingling, i.e. mixing funds from proceeds of crime with funds originating from legitimate business activities with the objective of obscuring the original source of these funds.
g. Use of false identities, i.e. transactions conducted with the use of false identities in an attempt to impede the tracing of identity and detection of money laundering.

B. Terrorism Financing

1. Terrorism financing is the direct or indirect use of assets for terrorism activities. In classification of crime, terrorism financing is essentially different from Money Laundering. Nevertheless, the two types of crime share similarities in the use of financial services as a vehicle for committing crime.
2. Unlike Money Laundering, which has the objective of disguising the origin of assets, terrorism financing seeks to aid terrorist

activities, whether with assets constituting proceeds of crime or with legitimately acquired assets.

3. To prevent Providers from being exploited as a vehicle for crimes of terrorism financing, each Provider needs to implement the AML and PTF Programme in an adequate manner.

C. Policies for Implementation of the AML and PTF Programme

1. To prevent Providers from being exploited as vehicles for money laundering and/or terrorism financing, Providers are required to implement the AML and PTF Programme.

2. The AML and PTF Programme is integral to the implementation of prudential principles for Providers, which encompass at least the following:
   a. Responsibilities of the Board of Directors and active oversight by the Board of Commissioners;
   b. Policies and procedures;
   c. Internal control; and
   d. Human resources.

3. In implementing the AML and PTF Programme, Providers are required to have written policies and procedures in place encompassing at least:
   a. implementation of CDD and EDD, consisting of:
      1) requesting information and documents;
      2) verification of documents; and
      3) monitoring of transactions.
   b. administration of documents;
   c. ascertaining of user profiles and updating of information on users;
   d. refusal and termination of business dealings;
   e. policy and procedures for funds transfers; and
   f. reporting to PPATK.

4. The above policies and procedures shall be set forth in AML and PTF Guidelines and must take account of the factor of potential misuse of information technology by money launderers or financers of terrorism, including at times when the Provider releases new products or services.

5. These AML and PTF Guidelines must be communicated to all employees and applied on a consistent and sustained basis for effective implementation of the AML and PTF programme.

D. Reporting to the Financial Transaction Reporting and Analysis Centre (PPATK)

Providers are required to submit the following to PPATK:

1. Suspicious Transaction Reports (STRs).
   The elements of Suspicious Transaction as stipulated in the AML Law are as follows:
   a. Transactions in departure from the profile, characteristics or customary nature of transactions by the user concerned;
   b. Transactions by users reasonably suspected for the purpose of circumventing the requirement for the reporting party concerned to report the transaction in accordance with the provisions of the AML Law.
   c. Transactions conducted or cancelled using assets suspected to constitute proceeds of crime; and
   d. Transactions requested by PPATK to be reported by the reporting party by reason of involving assets suspected to comprise proceeds of crime.

2. Cash Transaction Report (CTR):
   The information that must be reported in the CTR is Cash Transactions in amounts of no less than Rp 500,000,000.00 (five hundred million rupiahs) or equivalent amount in foreign currency, whether conducted in a single transaction or in multiple transactions on 1 (one) working day.

Transactions …

Transactions are defined as transactions for executing or receiving placement, deposit, withdrawal, book-keeping transfer, transfer, payment, grant, donation, safekeeping and/or exchange of a sum of money or other money-related action and/or activity.

Cash Transaction is defined as a Transaction conducted with the use of banknotes and/or coins.

3. Incoming and outgoing international funds transfer Transactions.

   Transactions that must be reported in regard to incoming and outgoing international funds transfers are stipulated by PPATK.

The reporting procedure shall follow the guidelines issued by PPATK.

CHAPTER II …

CHAPTER II

MANAGEMENT

Support for implementation of the AML and PTF Programme necessitates responsibilities to be assigned to the Board of Directors and active oversight conducted by the Board of Commissioners, in addition to establishment of a specialist unit and/or appointment of an officer responsible for implementation of the AML and PTF Programme.

A. Responsibilities of the Board of Directors and Active Oversight by the Board of Commissioners

1. Responsibilities of the Board of Directors

   The responsibilities of the Board of Directors shall encompass at least the following:

   a. Establishment of written policies and procedures for implementation of the AML and PTF programme pursuant to approval by the Board of Commissioners.
   b. Ensure that the AML and PTF programme is implemented in conformity with the established written policies and procedures.
   c. Ensure that written policies and procedures for the AML and PTF programme are aligned to changes and developments in products, services, technology, modus of money laundering or terrorism financing and to the applicable regulatory provisions relevant to the AML and PTF programme.
   d. Ensure the submission of STRs, cash transactions and incoming and outgoing international transactions to PPATK in accordance with laws and regulations.
   e. Ensure that all employees are informed and/or receive training about the implementation of the AML and PTF programme, and

f. Ensure …

f. Ensure the updating of customer profiles and customer transaction profiles.

2. Active Oversight by the Board of Commissioners
   a. Approval of policies for implementation of the AML and PTF programme; and
   b. Oversight of the discharge of responsibilities of the Board of Directors in regard to implementation of the AML and PTF programme.

B. Specialist Unit

1. Establishment of Specialist Unit
   a. Providers are required to establish a Specialist Unit (SU) responsible for implementation of the AML and PTF programme.
   b. If on the basis of the workload and complexity of business of the Provider, it is not possible to establish an SU, the Provider is required to appoint at least one employee responsible for implementation of the AML and PTF programme.

      Responsibility for implementation of the AML and PTF programme may be held by an employee concurrently with other duties insofar as these duties do not pertain to operations and/or oversight of implementation of the AML and PTF programme. Operational staff is defined as employees serving Users and/or prospective Users, including but not limited to tellers or customer service. Supervisors of implementation of the AML and PTF programme include but are not limited to employees of the internal audit unit.
   c. If a Provider is unable to establish an SU and is unable to appoint an employee responsible for implementation of the AML and PTF programme, the responsibility for

implementation ...

implementation of the AML and PTF programme shall be discharged by a member of the Board of Directors.

2. Organisational Structure

   a. In carrying out its duties, the SU or designated employee shall report to and be responsible to the competent Director.
   b. The SU or designated employee shall coordinate implementation of the AML and PTF programme in all operational units, including branch offices.

3. Duties and Responsibilities

   The principal duties of the SU or officer responsible for implementation of the AML and PTF Programme are:

   a. monitor the operation of systems supporting the AML and PTF programme, including but not limited to developing a suitable mechanism for communication from the operational units or relevant employees to the SU or employee responsible for implementation of the AML and PTF programme, while ensuring confidentiality of information (anti-tipping off);
   b. monitor the updating of User profiles and User transaction profiles;
   c. monitor to ensure that policies and procedures are aligned to the latest developments in the AML and PTF programme, the product risks of the Provider, the activities and complexity of the business conducted by the Provider and the transaction volume of the Provider;
   d. receive and analyse reports from operational units of potentially suspicious transactions;
   e. prepare STRs and other reports as referred to in the AML Law for submission to PPATK;
   f. monitor areas of high risk in regard to potential for money laundering or terrorism financing with reference to the

applicable …

applicable regulatory provisions and adequate sources of information; and

g. perform the role of contact person for the competent authorities pertaining to implementation of the AML and PTF programme, including but not limited to Bank Indonesia, PPATK and law enforcement agencies.

4. Requirements and Authorisations

a. Employees of the SU or the employee responsible for implementation of the AML and PTF programme must possess adequate knowledge and capacity concerning AML and PTF in addition to other regulations pertaining to the services of the payment system; and

b. Employees of the SU or the employee responsible for implementation of the AML and PTF programme must be duly authorised to access all User data and other information pertaining to the performance of their duties.

CHAPTER III …

CHAPTER III

POLICIES AND PROCEDURES FOR CDD AND EDD

A. Overview of CDD and EDD Policies and Procedures

Customer Due Diligence (CDD) is an activity comprising the identification, verification and monitoring by the Provider to ensure that transactions are conducted in accordance with the relevant User profile. If the Provider has dealings with a User classified high-risk in regard to the possibility of money laundering and terrorism financing, the Provider must apply a more in-depth procedure for CDD known as Enhanced Due Diligence (EDD).

1. Providers are required to apply the CDD procedure when:
   a. engaging in business dealings with Users or prospective Users; or
   b. in doubt of the truthfulness of identity information provided by User, prospective User and/or Beneficial Owner.

2. Providers are required to conduct CDD for existing Users predating the enactment of this Circular Letter of Bank Indonesia if:
   a. transactions exist in significant amounts;
   b. fundamental changes have occurred in the standard of documentation;
   c. significant change has occurred in pattern of transactions; and/or
   d. information in the User profile is incomplete, if the Provider administers data on the User.

3. Providers are required to conduct the EDD procedure if a prospective User or User:
   a. is classified high-risk, including a Politically Exposed Person (PEP);

b. is …

b. is suspected to be conducting suspicious activities or transactions related to money laundering or terrorism financing; and/or

c. conducts transactions in the rupiah currency and/or foreign currency in an amount no less than or equal to Rp 100,000,000.00 (one hundred million rupiahs).

If the EDD findings identify a clear basis/reason for the transaction, monitoring of the transaction shall proceed as usual. However, if no clear reason can be ascertained, the transaction must be placed under tighter monitoring.

4. Determination of high risk shall be guided by the PPATK regulations prescribing guidelines for providers of financial services concerning identification of products, Users, business and countries classified as high-risk and guidelines for providers of financial services concerning identification of suspicious transactions pertaining to terrorism financing.

5. Providers are required to conduct EDD as referred to in the above number 3 by conducting CDD and the following activities:
   a. request additional information necessary to ascertain the truthfulness of the prospective User profile;
   b. request additional supporting documents to obtain assurance of the truthfulness of information concerning identity and sources of funds.
   c. conduct regular analysis at least of information of sources of funds, purpose of transactions and business dealings with related parties; and
   d. monitor the pattern of transactions more strictly in order to update the profile of the User or Beneficial Owner.

6. Providers must be vigilant for transactions or business dealings with Users that have ties to countries that have not adequately implemented the recommendations of the Financial Action Task

Force (FATF), for example, Prospective Users who have business partners in countries meeting the criteria of high-risk.

7. Providers must refuse provision of services to prospective Users who:
   a. do not possess legitimate identity documents;
   b. are unable to provide legitimate identification of the Beneficial Owner;
   c. are unable to provide adequate information for development of a User profile; and/or
   d. are suspected to use fictitious names or are unwilling to provide a name (anonymous).

8. Providers shall document any User who is refused service as referred to in the above number 7 in a dedicated register and report such User in an STR if the transactions of that User are implausible or suspicious.

B. Policy and Procedures in Identification

The written policies and procedures for identification of Users and prospective Users shall encompass at least the following:

1. Identification of prospective Users and Users in a manner commensurate to the level of risk of occurrence of money laundering or terrorism financing. If a prospective User or a User is identified as high-risk, the Provider shall conduct EDD.

2. For the purposes of identification of prospective Users and Users, the Provider shall request information, identity documents and supporting documents from the prospective Users and Users.

3. The scope of request for information covers:
   a. identity of prospective Users and Users;
   b. identity of Beneficial Owner, if a User has a Beneficial User;
   c. value and date of transactions, except for Users conducting transactions of the nature of receipt; and

d. other …

d. other information enabling the Provider to ascertain the User profile, as may be necessary.

C. Requests for Information

1. In the event that a User is other than a natural person (entity/ institution), the Provider must undertake the identification of the entity/institution concerned and of its Beneficial Owner.

2. The information that must be requested of a prospective User for the purposes of CDD encompasses at least the following:

Table 1. Information on prospective Users for CDD

No.	Natural Person	Other than Natural Person		
		Non-Incorporated Business Entity	**Legal Entity (including Foundation and Incorporated Association)**	**Government/ Statutory Agency**
1.	Full name, including any alias	Name of the non-incorporated business entity	Name of legal entity	Name of statutory/ government agency
2.	Identity document number	Number of business licence issued by the competent agency	Number of licence or approval as a legal entity, issued by the competent agency	
3.	Home address listed on identity card	Address of domicile	Address of domicile	Address of domicile
4.	Most recent home address, including telephone number if any			
5.	Place and date of birth	Place and date of establishment	Place and date of establishment	
6.		Taxpayer ID Number (NPWP)	Taxpayer ID Number (NPWP)	
7.		Identity of natural person acting for and on behalf of the User	Identity of natural person acting for and on behalf of the User	Identity of natural person acting for and on behalf of the User

No.	Natural Person	Other than Natural Person		
		Non-Incorporated Business Entity	**Legal Entity (including Foundation and Incorporated Association)**	**Government/ Statutory Agency**
8.		Power-of-Attorney or other legal document assigning legal power, for person acting for and on behalf of the User	Power-of-Attorney or other legal document assigning legal power, for person acting for and on behalf of the User	Power-of-Attorney or other legal document assigning legal power, for person acting for and on behalf of the User
9.	Nationality			
10.	Gender			
11.	Occupation and/or name of agency/ company and position			
12.	Identify of Beneficial Owner, if any	Identify of Beneficial Owner, if any	Identify of Beneficial Owner, if any	
13.	Other information enabling the Provider to ascertain the User profile, if necessary	Other information enabling the Provider to ascertain the User profile, if necessary	Other information enabling the Provider to ascertain the User profile, if necessary	Other information enabling the Provider to ascertain the User profile, if necessary

3. The information that must be requested of prospective Users for EDD as referred to in item A.3 covers, at a minimum, the information described in number 2 in addition to information on sources of funds, sources of income and the purpose and objective of the transaction.

D. Provision of Information in Processing Funds Transfers

In order to obtain information on the identity of Sending Users and ensure that this information is complete, the following provisions apply:

1. A forwarding Provider or receiving Provider is required to obtain and ensure the completeness of information on the identity of any Sending User.
2. The scope of information on Users as referred to in number 1 shall encompass at least:
   a. name; and
   b. account number, other unique reference number, address, identity document number or information on place and date of birth.
3. To ensure the completeness of information on the identity of a Sending User as referred to in number 1, a Forwarding Provider or Receiving Provider may request information on a Sending User from a Sending Provider.
4. Request for information as referred to in number 3 must be made in writing by an authorised officer, whether by letter or electronic media.
5. Inter-Provider requests and provision of information as referred to in number 3 shall be confidential and used only for the purpose of implementing the AML and PTF programme.
6. Requests for and provision of information must be documented by the Provider.

E. Requests for Documents

1. For Users who are natural persons, the information in the above table 1 must be supported by valid identity documents bearing a photograph of the bearer and issued by a competent authority.
   Examples of User identity documents for natural persons of Indonesian nationality are the Identity Card (KTP), Driving Licence (SIM), passport or other document bearing a photograph of the User. If necessary, a Provider may request supporting documents including but not limited to the Taxpayer ID Number (NPWP) card or Family Card (KK).

2. For ...

2. For Users comprising non-incorporated business entities, the identity document that must be requested is the business licence or other licence from a competent authority.

   Examples of User identity documents for a business entity not incorporated as a legal entity include a Trading Licence (SIUP), certificate of domicile or Business Location Permit (SITU).

3. For Users incorporated as legal entities, the identity documents that must be requested are:
   a. deed of incorporation and/or articles of association of the legal entity, validated by the competent agency; and/or
   b. business licence or other licence from a competent agency, for example, a business licence from Bank Indonesia to operate as Money Changer or as provider of CBPI.
4. For a prospective User comprising a Statutory Agency or Government Agency, the identity document that must be requested is the letter of appointment for the party representing the agency for business dealings with the Provider.

F. Document Verification

1. Information provided by a prospective User and its supporting documents must be examined for authenticity through verification of the identity document and supporting documents to ascertain that the information is true and up to date. In case of any doubt, verification shall be undertaken on the basis of credible documents and/or other sources of information.

2. In order to obtain assurance of the authenticity of identity of a prospective user, verification shall be performed by:
   a. Checking the likeness of the prospective User to the photograph on the identity card.
   b. Examination of the authenticity of identity documents and supporting documents.

c. Requesting …

c. Requesting the prospective User to provide more than one identity document or supporting document issued by a competent authority, if doubts arise over the existing identity card.

d. Completion of identity verification process for the prospective User before engaging in business dealings with the prospective User.

e. Face-to-face meeting with the prospective User in the first instance of business dealings with the Provider.

   If the Provider uses the findings of CDD performed by a third party, the Provider shall not be required to meet face-to-face if a face-to-face meeting has previously been conducted by that third party.

   The meaning of "third party" is any party comprising a reporting party as referred to in the laws and regulations concerning prevention and eradication of money laundering.

f. If necessary, the prospective User may be interviewed to obtain assurance of the legitimacy and authenticity of the information, proof of identity and supporting documents of the prospective User.

g. If necessary, cross checks may be made to ascertain the consistency of various information provided by the User, including but not limited to:

   1) contacting the User by telephone (home or office);
   2) contacting a human resources officer in the place of employment of the User, if the occupation of the User is employee of a company or government agency; or
   3) obtaining confirmation of the income of the User by requiring evidence of deposits held by the User in a Bank domiciled in Indonesia.

h. For the purposes of verification, the Provider may also check the name of a prospective User against the Terrorist List. The Terrorist List is a list of names of terrorists

recorded …

recorded under United Nations (UN) Security Council Resolution 1267.

Information on the Terrorist List can be obtained, among others, from the UN website:
http://www.un.org/committees/1267/consolist.shmtl

G. Monitoring

1. To identify the appropriateness of User transactions to User profile, the Provider shall conduct monitoring subject to the following provisions:
   a. conducted on an ongoing basis, using a risk-based approach; and
   b. conducted through analysis of all transactions in departure from the User profile, with attention to transactions that are complex, high value and not of a customary nature, or transactions without an economic interest.
2. The monitoring of User profile and transactions on an ongoing basis encompasses the following activities:
   a. ensuring the completeness of User information and documents;
   b. examining the appropriateness of the transaction profile to the User profile; and
   c. examining the similarity or matches of the User name with the names listed in the terrorist list database issued by the competent authorities, including but not limited to the UN, and names of suspects or persons charged, as determined by the competent authorities.

      Information on the Terrorist List can be obtained, among others, from the UN website:
      http://www.un.org/committees/1267/consolist.shmtl
3. The Provider may ask the User for information concerning the background and purpose of a transaction in respect of a

transaction ...

transaction in departure from the User profile, taking into account anti-tipping off provisions stipulated in the AML Law.

4. If the results of monitoring indicate a similarity or match of names as referred to in the above item 2.c, the Provider must obtain clarification from the User to ascertain this similarity.

5. If the name and identity of the User match the name of a suspect or charged person and/or the terrorist list as referred to in item 2.c, the Provider must report the User in an STR.

6. Monitoring of a User must be tightened, among others, if the following are discovered:
   a. high-risk incoming or outgoing international remittance transaction; or
   b. transaction conducted by the User classified as PEP.

   Monitoring may be tightened by increasing the frequency of monitoring.

7. All monitoring activities shall be documented on an orderly basis.

H. Enhanced Due Diligence (EDD)

1. EDD or more in-depth activities of CDD must be performed for high-risk Users, including PEPs.

2. The nature, quality and quantity of User information that needs to be obtained must portray the level of risk arising from business dealings that take place.

3. Information obtained must be verifiable and provide assurance of the true profile of the User.

4. From a prospective User:
   a. request additional information as necessary to ascertain the profile of the prospective User; and/or
   b. request additional supporting documents to obtain assurance of the authenticity of information concerning

identity, sources of funds, sources of income and the purpose and objective of the transaction.

5. For a User or Beneficial Owner:
   a. conduct activities such as those conducted for a prospective User as referred to in number 4;
   b. conduct regular analysis at least of information concerning identity, sources of funds, sources of income and the purpose and objective of a transaction; and
   c. monitor the pattern of transactions by the customer more closely to ensure the plausibility of a transaction.

I. Updating

1. Providers are required to update User documents, data and information.
2. Updating of User documents, data and information as referred to in number 1 shall take place applying a risk-based approach.
3. The risk-based approach shall be applied, among others, by taking into account the following:
   a. level of risk of the country of destination or country of origin of the transaction;
   b. level of risk of the User, for example, a User classified as PEP; and
   c. occurrence of transactions in significant amounts and/or in departure from the transaction profile or User profile.
4. All activities for updating data must be documented in an orderly manner.

J. CDD by Third Parties

1. Providers may use the results of CDD conducted by a third party. If there is any doubt, the Provider must undertake identification and verification of the results of the CDD conducted by the third party, for example, by cross-checking the

name of a prospective User. The ultimate responsibility for the outcome of identification and verification and any decision to engage in business dealings with a User constitutes the responsibility of the Provider.

2. A third party as referred to in number 1 is a reporting party in accordance with the regulatory provisions concerning Anti-Money Laundering and Prevention of Terrorism Financing.

3. The results of CDD that may be used by a Provider are results of CDD from a third party meeting at least with the following criteria:
   a. has a CDD procedure that complies with the applicable regulatory provisions;
   b. has cooperation with the Provider in the form of a written agreement;
   c. is domiciled in a country that has implemented the FATF recommendations; and
   d. is willing to comply with requests for information at least concerning:
      1) full name as stated on the identity card;
      2) address and place and date of birth;
      3) number of identity card; and
      4) nationality of prospective User,

      and copies of supporting documents, if at any time required by the Provider as part of implementation of the AML and PTF programme. This willingness shall be set forth in the written agreement referred to in letter b.

4. If when conducting CDD, the Provider cooperates with another party that is not a reporting party (including outsourcing or an agent), the performance of CDD activities by that other party shall be deemed part of the CDD performed by the Provider itself. Accordingly, the other party does not constitute a third party as referred to in numbers 1 and 2. In this event, the Provider shall

continue ...

continue to bear full responsibility for the performance of CDD by that other party and shall ensure its compliance with the applicable regulatory provisions.

5. Providers are responsible to administer documents of the results of CDD conducted by third parties, data of the results of identification and verification as referred to in number 1 and documents for the results of CDD conducted by the Provider itself through other parties not comprising reporting parties (including outsourcing or agents).

K. Beneficial Owners

1. Providers are required to ascertain whether a prospective User or a User is acting on behalf of a Beneficial Owner in conducting business dealings with the Provider.

2. In the event that a prospective User or User is acting on behalf of a Beneficial Owner, the Provider is required to apply all CDD and EDD procedures to the prospective User or User and Beneficial Owner.

3. In the event that a Beneficial Owner is categorised as a Politically Exposed Person (PEP), the procedure to be applied is the EDD.

4. Providers are required to obtain the same identity documents and/or supporting documents for information of a Beneficial Owner as for documents for a prospective User as referred to in Table 1, with the addition of the following documents:

Table 2. Documents and other information pertaining to Beneficial Owners (BO)

No.	BO of Natural Person User	BO of Business User Not Incorporated as Legal Entity	BO of User Incorporated as Legal Entity
1.	Documents indicating a relationship or linkage	Document appointing a person as the	Document appointing a person

between ...

No.	BO of Natural Person User	BO of Business User Not Incorporated as Legal Entity	BO of User Incorporated as Legal Entity
	between the prospective User and the Beneficial Owner, as demonstrated among others by letter of appointment, power of attorney or other document	Beneficial Owner of the User, demonstrated among others by a written declaration.	as the Beneficial Owner of the User, demonstrated among others by articles of association, deed of incorporation or written declaration.
2.	Written declaration from the prospective User concerning the authenticity of identity and sources of funds of the Beneficial Owner	Written declaration from the prospective User concerning the authenticity of identity and sources of funds of the Beneficial Owner	Written declaration from the prospective User concerning the authenticity of identity and sources of funds of the Beneficial Owner

5. The obligation to provide documents for a Beneficial Owner as referred to in number 4 does not apply to government agencies or companies listed on the stock exchange. A Beneficial Owner that benefits from this waiver is notwithstanding required to provide documentation by recording the identity of the Beneficial Owner.

6. If the Provider is in doubt or unable to obtain certainty of the identity of the Beneficial Owner, the Provider is obliged to refuse business dealings or transactions with the prospective User.

L. High-Risk Users and PEPs

1. Providers are required to identify prospective Users, Users and/or Beneficial Owners who fulfil the criteria of high-risk and/or PEP.

2. Providers must put together a list of Users who are PEPs in a separate list.

3. In conducting business dealings with high-risk Users and/or PEPs, the Provider must appoint a senior officer with knowledge and experience of AML and PTF as the competent officer to:
   a. approve or reject a prospective User that is high-risk and/or a PEP; and/or
   b. decide whether to continue or terminate business dealings with a User or Beneficial Owner that is high-risk and/or a PEP.

M. Establishment of Criteria for High-Risk Areas

When categorising Users by level of risk, the Provider may apply the guidelines of the PPATK regulations that prescribe Guidelines for Identification of High-Risk Products, Users, Businesses and Countries for Providers of Financial Services, hereafter referred to as PPATK Identification Guidelines.

The high-risk areas in these guidelines are not only based on the PPATK Identification Guidelines, but also other references issued by competent authorities or that have become customary international practice.

1. High-Risk Products and Services

   In general, the characteristics of high-risk products and high-risk services are products/services offered to Users that are easily converted into cash or cash equivalent, or for which the funds are easily moved from one jurisdiction to another jurisdiction for the purpose of obscuring the origin of the funds.

2. High-Risk Users

   Among high-risk users are PEPs entrusted to hold public functions, including bearers of state office as referred to in the laws and regulations governing bearers of state office and/or persons listed as members of any political party who exerts influence on the policy and operations of the political party, whether of Indonesian nationality or foreign nationality. For

PEPs ...

PEPs comprising bearers of state office in Indonesia, the criteria are as follows:

Table 3. Criteria for PEPs

Legal Provision	Definition	Remarks
Act No. 28 of 1999 concerning Clean Bearers of State Office Untainted by Corruption, Collusion and Nepotism	State Officials performing executive, legislative or judicial functions and other officials whose functions and key duties pertain to the state office in accordance with the applicable provisions of laws and regulations.	• State Official at a Supreme Institution of State; • State Official at a High Institution of State; • Minister; • Governor; • Judge; • Other state official according to the provisions of laws and regulations; and • Other official holding a strategic function in relation to state office according to the provisions of applicable laws and regulations, including but not limited to board of directors of an SOE and board of directors of a Regional Government Enterprise.
Circular Letter SE/03/ M.PAN/01/2005 dated 20 January 2005 concerning Disclosure of Assets Owned by Bearers of State Office.	Bearers of State Office	• Echelon II official and other official of equivalent standing at a government agency and/or statutory agency. • All heads of offices under the Ministry of Finance • Supervisors of Customs and Excise; • Auditors; • Officials issuing licensing; • Officials/Heads of Public Service Units; and • Officials responsible for regulatory development

Parties classified as PEPs also include:

a. companies owned or managed by a PEP;

b. relatives ...

b. relatives of PEPs to the second degree; and/or
c. parties who in a general sense are publicly known to have close ties with PEPs.

3. High-Risk Business

Examples of high-risk business include but are not limited to the following:

a. securities dealers operating as stock brokers (corporate customers);
b. insurance companies and insurance brokers (companies);
c. money changes (companies);
d. pension funds and business funding (companies);
e. entertainment facilities and executive clubs;
f. remittance services;
g. accountancy, legal and notarial services (companies/natural persons);
h. surveyor services and real estate agents (companies);
i. precious metals dealer (companies/natural person);
j. dealers of antique goods, car dealers, dealers of ships and vendors of luxury goods; or
k. travel agents.

4. User transactions pertaining to other high-risk countries.

Examples of high-risk countries include, but are not limited to:

a. country in which the implementation of FATF recommendations is identified as inadequate;
b. included in the FATF statement list;
c. widely known to be a place of narcotics production and centre of the narcotics trade;
d. widely known to apply strict banking secrecy laws;
e. known to be a tax haven, among others on the basis of recent data from the Organisation for Economic Cooperation and Development (OECD). In May 2009, 35

countries ...

countries and territories were categorised as tax havens as follows:

1. Aruba	13. Grenada	25. Samoa
2. Anguilla	14. Guernsey	26. Panama
3. Antigua and Barbuda	15. Isle of Man	27. San Marino
4. Bermuda	16. Jersey	28. Seychelles
5. Bahamas	17. Liberia	29. St. Lucia
6. Bahrain	18. Malta	30. St. Kitts & Nevis
7. Belize	19. Marshall Islands	31. St. Vincent and the Grenadines
8. British Virgin Islands	20. Mauritius	32. Turks & Caicos Islands
9. Cook Islands	21. Montserrat	33. US Virgin Islands
10. Cyprus	22. Niue	34. Vanuatu
11. Dominica	23. Nauru	35. Cayman Islands
12. Gibraltar	24. Netherlands Antilles	

f. are known to have high levels of corruption. This information can be obtained, among others, from the publications of Transparency International; or

g. are subject to UN sanctions.

CHAPTER IV

RISK-BASED APPROACH

1. The risk profile depicts the level of risk of a User, product or services with potential for money laundering or terrorism financing, including but not limited to remittance services or bank products using electronic services.
2. Risk-based identification of Users may be performed by taking into account the following:
   a. User identity;
   b. Business address/location of the User;
   c. User profile; and
   d. transaction value.

Table 4. Sample classification of risk profile

	Low	Medium	High
User Identity	Presents more than one valid identity and is domiciled according to the address on the identity card.	Data/information on the identity of a prospective User has expired, but the User is cooperative with updating.	• User does not possess an identity issued by a competent authority. • Data/information on the identity of a prospective User is doubtful, for example, an identity card is issued by a competent authority, but the data is inaccurate, etc. • Identity data/ information does not match domicile, or the User constantly changes location or cannot be contacted.

Users …

	Low	Medium	High
			• Users of Indonesian nationality, who when opening an account use an address outside the territory of Indonesia.
User Business Address/ Location	Business address/ location in the same district/ municipality or bordering the district/ municipality in which [the Provider] is located.	Business address/ location outside the district/ municipality in which the Non-Bank Provider of Payment System Services is located.	Business address/ location of the User is in a free trade zone.
User Profile	Farmers/farm labourers	Company employees	• Persons classified high-risk in accordance with the guidelines specified in PPATK rules. • Employees of companies categorised high-risk.
	Vendors at traditional markets	Money changers or remittance services	Cash-based business, such as mini markets, parking attendants or lots, restaurants, filling stations, vendors of phone top-ups
Transaction Value	Low value transactions, e.g. below Rp 1,000,000.00 (one million rupiahs) and commensurate to the user profile.	Sizeable transactions, but supported by adequate documents or documents nevertheless deemed plausible or commensurate to the user profile.	Large cash transactions, e.g. more than Rp 100,000,000.00 (one hundred million rupiah) and/or not commensurate to the customer profile.

3. These …

3. These risk classifications do not apply to any User classified as PEP. Accordingly, if a prospective User or User is classified as PEP by reason of her/his occupation or official position, the person concerned shall automatically be classified high-risk.

CHAPTER V …

CHAPTER V

DOCUMENT ADMINISTRATION AND REPORTING

A. Document Administration

1. Providers are required to maintain proper document administration as a measure to assist the competent authorities in tracking funds with indications of originating from proceeds of crime. Accordingly, the documents held/archived by a Provider must be accurate and complete, enabling easy searching should this be necessary.
2. The documents to be administered cover at least the following:
   a. documents pertaining to information on prospective Users, Users or Beneficial Owners, including but not limited to identification (example: photocopy of identity card) and transaction information; and
   b. financial documents pertaining to Users, including but not limited to records, bookkeeping evidence and data on supporting financial administration constituting evidence of rights and obligations and the business of the Provider.
3. The retention periods for administering documents are as follows:
   a. for documents for the purpose referred to in item 2.a, not less than 5 (five) years after completion of the transaction and/or provision of services to the User;
   b. for documents for the purpose referred to in item 2.b, in accordance with the period referred to in the law governing corporate documents.
4. Documentation may be retained for a longer period if pertaining to a particular case and this retention is requested by a competent authority, such as Bank Indonesia or PPATK.

5. Documents ...

5. Documents may be administered in original form, copies, electronic form, microfilm or documents that based on the applicable law may be used as evidence.

6. Copies of identity documents shall be administered after authenticating the copy of the identity document with the original identity document.

B. Reporting

1. Providers are required to convey Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs) and other reports to PPATK as stipulated in the AML Law.

2. Other reports as referred to in the AML Law Article 23 paragraph (1) letter c, including but not limited to reports of incoming and outgoing international transactions.

3. Based on the results of monitoring the profiles and transactions of Users, the Provider is required to report information in a CTR if:
   a. A transaction meets the criteria of suspicious as stipulated in the AML Law;
   b. A User bears similarity or matches the name and identity of a suspect or person charged with crime and/or with the list of terrorists stipulated by the competent authority;
   c. Business dealings are terminated with a User due to unwillingness to provide information and supporting documents, and in the assessment of the Provider, the transactions conducted are implausible or suspicious; or
   d. Users and prospective Users are refused or their transactions are cancelled due to unwillingness to provide information requested by the Provider, and in the assessment of the Provider, the transactions conducted are implausible or suspicious.

4. Providers ...

4. Providers are required to submit a CTR to PPATK no later than 3 (three) working days after an element of an implausible or suspicious transactions comes to the attention of the Provider.

5. Providers are required to submit a CTR to PPATK no later than 14 (fourteen) working days commencing from the date of execution of a transaction.

6. Procedures for reporting suspicious transactions (including transactions suspected to have ties with terrorism or terrorism financing), cash transactions and other reports to PPATK are as stipulated in the PPATK Guidelines prescribing Guidelines for Providers of Financial Services concerning Identification and Procedure for Reporting Suspicious Transactions.

C. Record System

1. For the purpose of monitoring User profiles and transactions, Providers need to develop a records system capable of effectively identifying, analysing, monitoring and generating reports of the characteristics of transactions conducted by Users.

2. The records system in place must enable the Provider to trace each individual transaction, whether for internal purposes and/or for Bank Indonesia, and in regard to cases before court.

3. The sophistication of a records system for identifying suspicious transactions shall be commensurate to the complexity, transaction volume and risks of the Provider.

CHAPTER VI …

CHAPTER VI

INTERNAL CONTROL

1. Providers are required to have an effective internal control system operated under policies adopted by the Board of Directors concerning:
   a. limits of authority and responsibility of the relevant unit for implementation of the AML and PTF programme; and
   b. examination by the internal audit function of the effectiveness of implementation of the AML and PTF programme.
2. The meaning of effective internal control system is one capable of ensuring that the AML and PTF programme operates in compliance with established policies and procedures.
3. To ensure the effectiveness of AML and PTF programme implementation, a Provider may optimise the existing internal control unit or staff, including but not limited to conducting tests of compliance (including use of test transactions) with the policies and procedures pertaining to the AML and PTF programme.
4. Internal audit function officers must have powers to:
   a. access all documents pertaining to implementation of the AML and PTF programme;
   b. provide recommendations for remedial measures in respect of existing findings; and
   c. report to PPATK each suspicious transaction uncovered when conducting an audit and not reported to the SU or the designated officer.
5. The staff of the internal audit function must:
   a. have adequate facilities, including but not limited to an audit programme and procedures encompassing compliance

tests …

tests with focus on CDD and high-risk operations, products and services;

b. possess capacity and knowledge pertaining to AML and PTF;

c. conduct assessment of the adequacy of the processes in place at the Provider for identifying and reporting suspicious transactions; and

d. convey reports of examination findings to the Board of Directors and/or management on a timely basis.

CHAPTER VII

HUMAN RESOURCES AND EMPLOYEE TRAINING

A. Human Resources

1. A Provider is required to operate a screening process when recruiting new employees in order to prevent exploitation of the Provider as a vehicle or target of money laundering or terrorism financing involving the employees of the Provider itself.
2. The screening method shall be adjusted to the needs, complexity of activities and risk profile of the Provider.
3. The screening method shall operate, among others, by ensuring that candidates for employment do not hold any criminal record as stipulated in the money laundering law.
4. The Provider must monitor the profile of existing employees.

B. Training

1. Training Participants
   a. All employees must acquire knowledge of the policies, procedures and implementation of the AML and PTF programme. Priority for training shall be given to employees meeting the following criteria:
      1) meeting face-to-face with Users (services for Users);
      2) performing tasks related to oversight of AML and PTF programme implementation; or
      3) performing tasks related to reporting to PPATK and Bank Indonesia.
   b. Training as referred to in letter a shall be provided on a regular basis to employees who meet the above criteria. Other employees who do not meet the above criteria must receive training no less than 1 (one) time during their period of employment.

c. Employees …

c. Employees dealing face-to-face with Users must receive training before taking up their position.

2. Training Methods

Training may be conducted by:

a. provision of in-house training;
b. enrolling employees in training conducted by another party, whether in the form of workshop or seminar;
c. knowledge sharing, and/or
d. learning with the use of electronic media (e-learning) and in meetings.

3. Training Topics

Training topics shall cover at least the following:

a. implementation of the laws and regulations pertaining to the AML and PTF programme;
b. techniques, methods and typology of money laundering or terrorism financing, including trends and developments in the risk profile of payment system services; and
c. policies and procedures for implementation of the AML and PTF programme and the roles and responsibilities of employees in eradicating money laundering or terrorism financing, including consequences should an employee provide a tip-off about a Suspicious Transaction Report being put together or conveyed to PPATK.

CHAPTER VIII

ILLUSTRATIONS AND EXAMPLES

OF CASES OF SUSPICIOUS TRANSACTIONS

IN NON-BANK PROVISION OF PAYMENT SYSTEM SERVICES

A. Illustrative Cases of Suspicious Transactions

1. Illustrative Case of an ST in the Card-Based Payment Instrument Industry:

   Case:

   Shop X, a shop selling daily household needs, has an average daily turnover of Rp 5,000,000.00 (five million rupiahs). Over time, Shop X submits an application for cooperation to operate as a merchant of Acquirer A. Acquirer A grants this request and places one of its EDCs (Electronic Data Capturer) at the Shop X location. During the first 6 (six) months after placing the EDC, the daily turnover of Shop X rises to Rp 8,000,000.00 (eight million rupiahs). However, in the seventh and eight months, average daily turnover for Shop X climbs to Rp 20,000,000.00 (twenty million rupiahs). After a review, no change or addition could be found in the type and quantity of goods sold by Shop X.

   Suspicious Indicators:

   - Average daily turnover of PT X after becoming a user for Acquirer A was Rp 8,000,000.00 (eight million rupiahs) during a 6 (six) month period, and this increased drastically to Rp 20,000,000.00 (twenty million rupiahs) in the seventh and eighth months.
   - From available information, there was no change/addition in the type and capacity of goods sold by Shop X.

Elements …

Elements of ST:

The above series of transactions (daily turnover) is in departure from the business profile of the User (Shop X).

2. Illustrative Case of ST in Operation of Electronic Money Activities

Case:

Mr Y, a citizen of Jakarta, is the holder of Electronic Money issued by Issuer B. From the outset of his use of Electronic Money, Mr. Y had elected to use the registered type enabling him to hold a maximum value of Rp5,000,000.00 (five million) rupiahs) with cash withdrawal and funds transfer facilities. Under the Electronic Money regulations issued by Bank Indonesia, the maximum total use of electronic money during 1 (one) month is Rp20,000,000.00 (twenty million rupiahs). During the first 1 (one) year of use of the Electronic Money, all transactions conducted by Mr. Y were for payment of toll road charges in the Jakarta area, with average monthly use of Rp500,000.00 (five hundred thousand rupiahs). In the second year, Mr. Y made an additional purchase of 9 (nine) cards of new registered Electronic Money. With the 10 (ten) cards of Electronic Money held, Mr. Y conducted funds transfer and cash withdrawal transactions in the first month of the second year with a total value of Rp180,000,000.00 (one hundred and eighty million rupiahs). In addition, data held by the Issuer revealed that all cash withdrawal transactions were made with authorisation given to different third parties in various regions of Indonesia.

Suspicious Indicators:

- The initial use of electronic money held by Mr. Y was for payment of toll road charges with an average use of Rp500,000.00 (five hundred thousand rupiahs) per month. Mr. Y then made an additional purchase of a sum of

electronic …

electronic money for use in funds transfer and cash withdrawal transactions in large amounts.

- The cash withdrawals were made by different third parties outside the Jakarta area.

Elements of ST:

The above series of transactions fulfils the element of departure from the characteristics of the User.

3. Illustrative Case of ST in the Remittances Industry

Case:

Remittance Service Provider C is a Remittance Services company located in the Pasar Minggu area of South Jakarta. One day, a Ms. Z comes to the company with the purpose of transferring a sum of money overseas. The remittances that Ms. Z wishes to make are 6 (six) transactions, each with a value of Rp80,000,000.00 (eighty million rupiahs), bringing the total transaction value to Rp480,000,000.00 (four hundred and eighty million rupiahs). The transactions are in favour of 6 (six) different companies in Hong Kong, but with addresses near each other (same street address, differing only in the number). Furthermore, information comes to light that Ms. Z is domiciled in the Kelapa Gading area and works for an export-import company in Tanjung Priok.

Suspicious Indicators:

- Transaction of relatively large value for one conducted through the remittance service.
- Transaction in favour of different beneficiaries, but at nearby addresses.
- Total value of transactions just below the limit of Cash Transactions reportable to PPATK.
- The domicile and place of business of Ms Z is very far from the place of business of Provider C.

Elements …

Elements of ST:

The above series of transactions contain the following elements:

- Splitting of a transaction to avoid the requirement for reporting to PPATK;
- In departure from the profile for the user location.

B. SAMPLE ST CASES

1. Transactions with No Clear Economic Objective
   a. Credit Card Payments that result in a significant credit balance.
   b. Remittances not supported by adequate reason or in which no linkage exists between a remittance by a User and the business activity of the User.
2. Transactions Related to the Behaviour of the User or Transacting Party
   a. Use of many names to conduct transactions of a similar nature.
   b. Transfers to charitable organisations based overseas.
   c. Many similar transactions conducted on the same day in different locations.
   d. Third party is present throughout the transaction, but does not participate in conducting the transaction.
   e. User insists that the transaction be completed quickly.
   f. Transactions conducted by telephone or facsimile, or over the internet (non face-to-face).
   g. Incoming or outgoing international transfers in large amounts with instructions for payment in cash.
   h. Users arrive in a group at a Non-Bank Provider of Payment System Services but act as if strangers to each other, and then separately conduct transactions of similar nature.

i. Money in large amounts, but sources of funds that are doubtful or not consistent with the financial situation of the User.

j. User is unduly well-informed of the reporting requirements or internal control of the Non-Bank Provider of Payment System Services, its supervision and operational processes.

k. User provides inconsistent information to different employees of the same Non-Bank Provider of Payment System Services.

l. Detailed information about the User is unclear or difficult to verify.

m. User exhibits strong curiosity of something pertaining to a procedure for exemption.

n. User is secretive and avoids face-to-face meeting.

o. User provides excessive explanation of a transaction.

p. Questions put to the employee of the Non-Bank Provider of Payment System Services are not relevant or unreasonable.

q. User is hurried, panicky or nervous.

r. Information provided by the User contradicts information obtained from other sources.

s. User uses multiple addresses similar to each other.

t. Information of name, address or date of birth is inconsistent.

u. User refuses to provide explanations or attempts to conceal matters by changing the subject to other matters not pertaining to the transaction in question (large transaction conducted by the User within a certain period).

v. User refuses to answer questions during clarification of User data by an officer of the Non-Bank Provider of Payment System Services by asserting that the User is a prominent/important person or has close ties with officials in a certain region.

w. Pattern ...

w. Pattern of User transactions in departure from established habits, for example the User normally conducts transactions by courier and then switches to written orders.

x. Pattern of User transactions that are seldom or never conducted in cash suddenly switches to cash in very significant amounts.

y. User reported as involved in criminal acts (corruption, illegal logging, etc.), thus indicating that the funds originate from these acts.

z. User provides an implausible explanation of a cash remittance made in a very large amount.

3. Activities Categorised as Illegal

a. The User is reported in the media as a person suspected of involvement in illegal activities or crime.

b. Funds transfer instructions are received from a tax haven or country well known for terrorism financing.

4. Suspicious transactions involving employees of a Provider and/or its agents

a. Large increase in the wealth of an employee and/or agent of a Non-Bank Provider of Payment System Services without adequate explanation.

b. Transaction dealings through agents not accompanied by adequate information on the ultimate beneficiary.

5. Other Types of Transactions

a. Transaction activity out of character with the User Profile (e.g. age, occupation, income).

b. User frequently changes address and signature.

c. User insistently refuses to provide required information and documents or is willing to provide only minimum information, and/or provides information inconsistent with supporting documents.

CHAPTER IX ...

CHAPTER IX

GLOSSARY

Beneficial Owner: a person holding funds who controls the transactions of a User, issues authorisation for the event of a transaction and/or exercises control by means of a legal entity or agreement.

Cuckoo Smurfing: efforts to obscure original sources of funds by sending funds from proceeds of crime through accounts of third parties who wait for incoming remittances of funds and are unaware that the funds they receive constitute proceeds of crime.

Customer Due Diligence: is an activity comprising identification, verification and monitoring by a Non-Bank Provider of Payment System Services to ensure that transactions are conducted in accordance with the profile of a user of banking services.

Enhanced Due Diligence: CDD and other activities conducted by a Non-Bank Provider of Payment System Services to ascertain in-depth the profile of a prospective User, User or Beneficial Owner categorised high-risk, including a PEP, in regard to the possibility of money laundering and terrorism financing.

Financial Action Task Force (FATF): founded in 1989 by the G7 group of nations and tasked with assessing the results of existing international cooperation in prevention of exploitation of the banking system as a vehicle for money laundering, among others, by issuing comprehensive anti-money laundering standards.

Front Liner/Officer: officer of a Provider of Payment System Services dealing directly with Users requiring banking services, including but not limited to teller and customer service.

High-Risk Countries: states classified as high-risk for occurrence of money laundering or terrorism financing for reasons including but not limited to failure/delay in implementation of the FATF recommendations.

High-Risk ...

High-Risk Customer: Users classified as high-risk of being an actor/accessory in money laundering by reason of employment, position, the payment system service used or their business activity.

High-Risk Product: payment system product of considerable interest to money launderers.

Integration: attempts to make use of purportedly legitimate assets, whether for immediate benefit, investment in various material or financial assets, use in financing legal business activity, or to be ploughed back into criminal activity.

Legal Risk: risk arising from legal (juridical) weaknesses. Legal weaknesses include but are not limited to those arising from legal claims, absence of supporting laws and regulations or weaknesses in legal ties, such as failure to meet requirements for validity of a contract and flawed binding of collateral.

Mingling: the mixing of funds from proceeds of crime with funds from legitimate business activities with the objective of obscuring the original sources of the funds.

Money Laundering: the acts of placement, transfer, payment, expenditure, grant, donation, placing in safe-keeping, carrying overseas, exchange or other act in respect of assets known or reasonably suspected to constitute proceeds of crime for the purpose of concealing these assets or disguising their origin as purportedly legitimate assets.

Placement: attempts to place funds generated from a criminal activity into the financial system.

Politically Exposed Person: any person entrusted with holding public office, including any bearer of state office as defined in the laws and regulations concerning bearers of state office and/or any person registered as a member of a political party who exerts influences on the policies and operations of the political party.

Reputational …

Reputational Risk: risk including but not limited to that arising from publications of a negative nature pertaining to the business of a bank or negative perceptions of the bank.

Single Customer Identification File: User profile date encompassing all accounts held by a single User at a bank, including but not limited to savings deposits, time deposits, demand deposits and credit.

Smurfing: efforts to circumvent reporting by splitting transactions so that they are conducted by many parties.

Structuring: efforts to circumvent reporting by splitting transactions so that transaction amounts are smaller.

Suspicious Transaction: suspicious transaction as defined in the law concerning money laundering.

Tax Haven Country: a state or territory whose laws or policies can be exploited to circumvent or exploit loopholes in the taxation regulations of another state. The general criteria are: 1) no taxes, or only nominal level of taxation, 2) no exchange of taxation information with other states, 3) lack of transparency in the implementation of its laws and implementing regulations, 4) no obligation for foreign business entities to have a physical presence in that state, 5) promotion of the state or territory as an offshore financial centre and/or 6) a small state or territory with stable political conditions and economy, supported by good infrastructure.

Terrorist List: list of terrorist names recorded under US Security Council Resolution No. 1267.

Transfer (Layering): attempts to separate the proceeds of crime through financial transactions to conceal or disguise the origin of the funds. This activity involves a process of moving funds from a number of accounts or locations resulting from placement to other places through a complex series of transactions designed to disguise and eliminate traces of the source of these funds.

U-Turn …

U-Turn: attempts to obscure the origin of proceeds of crime by reversing a transaction so that it is subsequently returned to the account of origin.

HEAD OF THE DEPARTMENT
OF ACCOUNTING AND THE PAYMENT SYSTEM

(signed)

BOEDI ARMANTO